

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JIM O'DAY,

Plaintiff,

v.

NTT DATA AMERICAS, INC, and
NTT DATA SERVICES, LLC,

Defendants.

CIVIL ACTION NO.: 1 : 2 4 Civ. 5771 (VF)

**CONFIDENTIALITY STIPULATION
AND PROTECTIVE ORDER**

WHEREAS, the Parties having agreed to the following terms of confidentiality, and the Court having found that good cause exists for the issuance of an appropriately tailored confidentiality order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, it is hereby

ORDERED that the following restrictions and procedures shall apply to the information and documents exchanged by the parties in connection with the pre-trial phase of this action:

1. Counsel for any party may designate any document or information, in whole or in part, as confidential if counsel determines, in good faith, that such designation is necessary to protect the interests of the client in information that is proprietary, a trade secret or otherwise sensitive non-public information. Information and documents designated by a party as confidential will be stamped "CONFIDENTIAL."

2. The Confidential Information disclosed will be held and used by the person receiving such information solely for use in connection with the action.

3. In the event a party challenges another party's designation of confidentiality, counsel shall make a good faith effort to resolve the dispute, and in the absence of a resolution, the challenging party may seek resolution by the Court. Nothing in this Protective Order constitutes an admission by any party that Confidential Information disclosed in this case is relevant or admissible. Each party reserves the right to object to the use or admissibility of the Confidential Information.

4. The parties should meet and confer if any production requires a designation of "For Attorneys' or Experts' Eyes Only." All other documents designated as "CONFIDENTIAL" shall not be disclosed to any person, except:

- a. The requesting party and counsel, including in-house counsel;
- b. Employees of such counsel assigned to and necessary to assist in the litigation;

- c. Consultants or experts assisting in the prosecution or defense of the matter, to the extent deemed necessary by counsel; and
 - d. The Court (including the mediator, or other person having access to any Confidential Information by virtue of his or her position with the Court).
- 5. Prior to disclosing or displaying the Confidential Information to any person, counsel must:
 - a. Inform the person of the confidential nature of the information or documents;
 - b. Inform the person that this Court has enjoined the use of the information or documents by him/her for any purpose other than this litigation and has enjoined the disclosure of the information or documents to any other person; and
 - c. Require each such person to sign an agreement to be bound by this Order in the form attached as Exhibit A.
- 6. The disclosure of a document or information without designating it as “Confidential” shall not constitute a waiver of the right to designate such document or information as Confidential Information. If so designated, the document or information shall thenceforth be treated as Confidential Information subject to all the terms of this Stipulation and Order.
- 7. Any Personally Identifying Information (“PII”) (e.g., social security numbers, financial account numbers, passwords, and information that may be used for identity theft) exchanged in discovery shall be maintained by the receiving party in a manner that is secure and confidential and shared only with authorized individuals in a secure manner. The producing party may specify the minimal level of protection expected in the storage and transfer of its information. In the event the party who received PII experiences a data breach, it shall immediately notify the producing party of same and cooperate with the producing party to address and remedy the breach. Nothing herein shall preclude the producing party from asserting legal claims or constitute a waiver of legal rights and defenses in the event of litigation arising out of the receiving party’s failure to appropriately protect PII from unauthorized disclosure.
- 8. Pursuant to Federal Rule of Evidence 502, the production of privileged or work-product protected documents or communications, electronically stored information (“ESI”) or information, whether inadvertent or otherwise, shall not constitute a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). Nothing contained herein is intended to or shall serve to limit a party’s right to conduct a review of documents, ESI or information (including metadata) for relevance,

responsiveness and/or segregation of privileged and/or protected information before production.

9. Notwithstanding the designation of information as “Confidential” in discovery, there is no presumption that such information shall be filed with the Court under seal. The parties shall follow the Court’s procedures for requests for filing under seal.

10. At the conclusion of litigation, Confidential Information and any copies thereof shall be promptly (and in no event later than 30 days after entry of final judgment no longer subject to further appeal) returned to the producing party or certified as destroyed, except that the parties’ counsel shall be permitted to retain their working files on the condition that those files will remain protected.

11. Nothing herein shall preclude the parties from disclosing material designated to be Confidential Information if otherwise required by law or pursuant to a valid subpoena.

12. The Party or person producing or disclosing “Discovery Material” (i.e., information of any kind produced or disclosed in the course of discovery in this action) (the “Producing Party”) or its counsel may designate deposition exhibits or portions of deposition transcripts as Confidential Discovery Material either by: (a) indicating on the record during the deposition that a question calls for Confidential information, in which case the reporter will bind the transcript of the designated testimony in a separate volume and mark it as “Confidential Information Governed by Protective Order;” or (b) notifying the reporter and all counsel of record, in writing, within 30 days after a deposition has concluded, of the specific pages and lines of the transcript that are to be designated “Confidential,” in which case all counsel receiving the transcript will be responsible for marking the copies of the designated transcript in their possession or under their control as directed by the Producing Party or that person’s counsel. During the 30-day period following a deposition, all Parties will treat the entire deposition transcript as if it had been designated Confidential.

13. Absent notice to and written permission from the Producing Party, any person or entity authorized to have access to Designated Confidential Information under the terms of this Order shall not permit any Confidential or Highly Confidential Information to be used to train any artificial intelligence tool.

14. These restrictions apply to the use of advanced or generative AI tools from OpenAI’s GPT or ChatGPT, Harvey.AI, Google’s Bard, Anthropic’s Claude, and similar tools or applications.

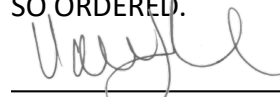
15. If the Receiving Party discovers a breach of security, including any actual or suspected unauthorized access, relating to another party’s Designated Confidential Information, the Receiving Party shall: (1) promptly provide written notice to Designating Party of such breach; (2) investigate and take reasonable efforts to remediate the effects of the breach, and provide Designating Party with assurances reasonably satisfactory to Designating Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Designating Party

can reasonably ascertain the size and scope of the breach. If required by any judicial or governmental request, requirement or order to disclose such information, the Receiving Party shall take all reasonable steps to give the Designating Party sufficient prior notice in order to contest such request, requirement or order through legal means. The Receiving Party agrees to cooperate with the Designating Party or law enforcement in investigating any such security incident. In any event, the Receiving Party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

SO STIPULATED AND AGREED.

Dated: New York, New York
July 21, 2025

SO ORDERED.



VALERIE FIGUEREDO

United States Magistrate Judge

The Clerk of Court is directed to terminate the motion
at ECF No. 23.

Exhibit A

Agreement

I have been informed by counsel that certain documents or information to be disclosed to me in connection with the matter entitled have been designated as confidential. I have been informed that any such documents or information labeled "CONFIDENTIAL" are confidential by Order of the Court.

I hereby agree that I will not disclose any information contained in such documents to any other person. I further agree not to use any such information for any purpose other than this litigation.

DATED:

Signed in the presence of:

(Attorney)